ROBBINS GELLER RUDMAN
& DOWD LLP
SHAWN A. WILLIAMS (213113)
Post Montgomery Center
One Montgomery Street, Suite 1800
San Francisco, CA 94104
Telephone: 415/288-4545
415/288-4534 (fax)
shawnw@rgrdlaw.com
– and –
PAUL J. GELLER
STUART A. DAVIDSON
JASON H. ALPERSTEIN
120 East Palmetto Park Road
Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)
pgeller@rgrdlaw.com
sdavidson@rgrdlaw.com
jalperstein@rgrdlaw.com

LABATON SUCHAROW LLP
JOEL H. BERNSTEIN
CORBAN S. RHODES
ROSS M. KAMHI
140 Broadway, 34th Floor
New York, NY 10005
Telephone: 212/907-0700
212/818-0477 (fax)
jbernstein@labaton.com
crhodes@labaton.com
rkamhi@labaton.com

Attorneys for Plaintiff Maria Corso

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

MARIA CORSO, Individually and on Behalf of All Others Similarly Situated, Plaintiff, vs. YAHOO! INC., Defendant.	Case No. CLASS ACTION COMPLAINT FOR GROSS NEGLIGENCE AND BAILMENT DEMAND FOR JURY TRIAL

Plaintiff Maria Corso ("Plaintiff"), individually and on behalf of all other similarly situated persons within Australia whose personal information was accessed following the data breach announced on September 22, 2016, by her undersigned attorneys, brings this class action complaint against defendants Yahoo! Inc. ("Yahoo," the "Company," or "Defendant") based on personal knowledge as to herself and upon information and belief as to all other matters based on the investigation of counsel.

NATURE OF THE ACTION

1. Yahoo is a leading Internet company that provides Internet-based services to hundreds of millions of users on a regular and consistent basis. Yahoo's services in Australia are provided by Yahoo!7 Pty Limited ("Yahoo7"), a joint venture between Yahoo and Seven Network Ltd.

2. As part of its business, Yahoo, through Yahoo7 in Australia, collects and stores large volumes of sensitive personal information about its users, including the users' names, email addresses, telephone numbers, birth dates, passwords, and security questions linked to a users' account. Yahoo requires all of this information in order to create an account.

3. Despite the fact that it requires, collects and stores sensitive personal information for hundreds of millions of users, the Company has failed to adequately protect its users or itself from data breaches. Indeed, Yahoo's security systems have been breached in the past, and the Company has demonstrated that it cannot adequately secure the personal information of its users.

4. Despite Yahoo's promises to "take[] your privacy seriously," to "limit access to personal information about you to employees who we believe reasonably need to come into contact with that information to provide products or services to you or in order to do their jobs," and to "have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you," Yahoo failed to live up to those promises when it failed to adequately protect is users' personal information.

5. Specifically, on September 22, 2016, Yahoo issued a press release in which it announced that a "recent investigation" confirmed that sensitive personal account information associated with at least ***500 million user accounts*** "was stolen from ***the company's network*** in late

2014 by what it believes is a state-sponsored actor." The stolen information included users' names, email addresses, telephone numbers, dates of birth, hashed passwords and, in some cases, encrypted or unencrypted security questions and answers. Reports indicate that ***this data breach was the largest from a single site in history***.

6. As a result of Defendants' failure to establish and implement basic data security protocols, contrary to Yahoo's guarantees, its users' personal information is now in the hands of criminals and/or enemies of the Western world, subjecting Plaintiff and the Class (as defined below) to the serious risk of identity theft in a wide variety of forms.

7. Worse yet, despite the fact that the attack took place in late 2014, Yahoo was so grossly negligent in securing its users' personal information that it says that it did not even discover the incident until the summer of 2016. In other words, Defendant's misconduct was so bad that it evidently allowed unauthorized and malicious access to Plaintiff's and Class members' personal information on Defendant's computer systems to continue unimpeded for ***nearly two years***.

8. Circumstantial evidence suggests that certain Yahoo insiders ***did*** know of the breach long before it was disclosed, but hid it from the public until after a $4.8 billion sale of the Company to Verizon was announced in July 2016. Verizon has stated that it did not learn of the breach until September 20, 2016, and commentators have noted that "Verizon might want to lower the price it is paying because it wasn't notified of the hack sooner and doesn't yet know the full liability Yahoo and Verizon would face from victims of the hack." Now countless media outlets reports that Yahoo CEO Marissa Mayer knew about the breach in July 2016, before telling Verizon that the Company had not been the subject of a breach.

9. Plaintiff and Class members must now take matters into their own hands to protect themselves from fraud. Indeed, although the Company has stated that the "ongoing investigation" suggests that the stolen information did not include payment card data or bank account information,[1] Yahoo has nevertheless encouraged its users to consider placing a "security freeze" (also known as a "credit freeze") on their credit file. A security freeze is designed to prevent potential creditors from

[1] Plaintiff does not state this as a definitive fact.

accessing an individual's credit file at the consumer reporting agencies without the individual's consent, and, according to Yahoo's notice to its users, costs roughly between $5 and $20 per freeze. Yahoo has offered no financial assistance to its users.

10. In addition, countless Yahoo users are reporting that Yahoo or its authorized technicians are demanding payment of several hundred dollars for 1-3 years of "security protection" in order to access their hacked, blocked accounts.

11. On September 25, 2016, as a direct result of Yahoo's misconduct alleged herein, Plaintiff was forced to pay $150.00 for one year of technology support to ensure that her computer and the information contained thereon are secure and protected.

12. Plaintiff brings this class action lawsuit on behalf of all Australia Yahoo account holders whose accounts were hacked against Yahoo for failing to adequately safeguard her and others' personal information. Plaintiff seeks judgment requiring Yahoo to remedy the harm caused by its misconduct, which includes compensating Plaintiff and Class members for resulting account fraud and for all reasonably necessary measures Plaintiff and Class members have had to take in order to identify and safeguard the accounts put at risk by Yahoo's grossly negligent security.

INTRADISTRICT ASSIGNMENT

13. A substantial part of the events or conduct that give rise to the claims in this action occurred in the county of Santa Clara, and as such this action is properly assigned to the San Jose Division of this Court.

PARTIES

14. Plaintiff Maria Corso is a natural person and a resident and citizen of Clearview, South Australia. Ms. Corso is one of the approximately 500 million Yahoo users worldwide whose personal information was stolen because Yahoo was reckless in failing to secure such information.

15. Defendant Yahoo is a Delaware corporation headquartered at 701 First Avenue, Sunnyvale, California 94089. Yahoo does business throughout the State of California and the United States. Yahoo maintains a substantial portion of its computer systems in California.

JURISDICTION AND VENUE

16. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d) ("CAFA"), because (i) the proposed Class consists of well over 100 members; (ii) the parties are diverse, as members of the proposed Class are citizens of a foreign state and Yahoo is a citizen of California; and (iii) the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs.

17. This Court has personal jurisdiction over Plaintiff because Plaintiff submits to the Court's jurisdiction. This Court has personal jurisdiction over Yahoo because it maintains its principal headquarters in California, regularly conducts business in California, and has sufficient minimum contacts in California. In addition, Plaintiff's claims arise out of Defendant's conducting and transacting business in California, and many of the actions giving rise to the Complaint took place in this District.

18. Venue is proper in this District pursuant to 28 U.S.C. §1391 because Yahoo is a resident of this District and is subject to this Court's personal jurisdiction. Yahoo is registered to conduct business throughout California, regularly conducts business in this District, and maintains an office in this District. In addition, the causes of action arose, in substantial part, in this District.

FACTUAL ALLEGATIONS

Company Background

19. Yahoo operates a host of Internet websites and services, including web portal, search engine and e-mail service, among others. In Australia, Yahoo7 provides such services to Australian citizens and account holders. Upon information and belief, the personal, private information supplied to Yahoo7 to create an Yahoo7 account is maintained by Yahoo, which enabled Australian Yahoo users to have their accounts hacked by the same individuals who hacked the accounts of United States users and users worldwide. To be sure, as alleged below, Yahoo has admitted that "the company's" network was hacked and all 500 million accounts worldwide were compromised.

20. Yahoo's security systems have been breached before. In July 2012, a group of hackers based in Eastern Europe breached Yahoo's security measures and extracted e-mail addresses

and passwords that were stored unencrypted within a Yahoo database. The hackers then posted these login credentials online, in an effort to expose Yahoo's lax security measures.

21. Yahoo guarantees its users that it will take certain specific steps to protect the personal, private information Yahoo requires an individual provide the Company in order to create an account. Specifically, Yahoo promises on its website and in its Privacy Policy:

- to "take[] your privacy seriously";
- to "limit access to personal information about you to employees who we believe reasonably need to come into contact with that information to provide products or services to you or in order to do their jobs"; and
- to "have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you."

The Security Breach

22. According to Yahoo, it first learned of a potentially massive data breach at some point during the summer of 2016, when hackers posted to underground online forums certain data that they claimed was obtained from Yahoo. It was not clear whether the data came from Yahoo itself (as opposed to a third-party service), and so Yahoo launched an investigation, but was unable to confirm whether the stolen data had originated from a breach at Yahoo.

23. Although the Company says that it did not find evidence that the stolen data came from its own systems, it did find evidence of a far more serious breach: according to Yahoo, in 2014, a state-sponsored actor stole account information associated with approximately 500 million Yahoo users.

24. On September 22, 2016, Yahoo issued a press release announcing that its internal investigation had confirmed that account information associated with ***at least 500 million user accounts*** had been stolen. The press release, admitting that Yahoo and not Yahoo7 stored the user data for all 500 million Yahoo account holders, stated, in part, as follows:

> A recent investigation ***by Yahoo! Inc.*** (NASDAQ:YHOO) has confirmed that a copy of certain user account information was stolen from ***the company's network*** in late 2014 by what it believes is a state-sponsored actor. The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers. The ongoing investigation suggests that stolen information did not include unprotected passwords, payment card data, or

> bank account information; payment card data and bank account information are not stored in the system that the investigation has found to be affected. Based on the ongoing investigation, Yahoo believes that information associated with ***at least 500 million user accounts*** was stolen and the investigation has found no evidence that the state-sponsored actor is ***currently in Yahoo's network***. Yahoo is working closely with law enforcement on this matter.
>
> Yahoo is notifying potentially affected users and has taken steps to secure their accounts. These steps include invalidating unencrypted security questions and answers so that they cannot be used to access an account and asking potentially affected users to change their passwords. Yahoo is also recommending that users who haven't changed their passwords since 2014 do so.
>
> Yahoo encourages users to review their online accounts for suspicious activity and to change their password and security questions and answers for any other accounts on which they use the same or similar information used for their Yahoo account. The company further recommends that users avoid clicking on links or downloading attachments from suspicious emails and that they be cautious of unsolicited communications that ask for personal information. Additionally, Yahoo asks users to consider using Yahoo Account Key, a simple authentication tool that eliminates the need to use a password altogether.
>
> Online intrusions and thefts by state-sponsored actors have become increasingly common across the technology industry. Yahoo and other companies have launched programs to detect and notify users when a company strongly suspects that a state-sponsored actor has targeted an account. Since the inception of Yahoo's program in December 2015, independent of the recent investigation, approximately 10,000 users have received such a notice.

25. Numerous articles discussing the data breach immediately followed. Indeed, *The New York Times* published an article that same day, titled "Yahoo Says Hackers Stole Data on 500 Million Users in 2014," which quoted security experts who explained that the Yahoo data breach could have major consequences:

> "The stolen Yahoo data is critical because it not only leads to a single system but to users' connections to their banks, social media profiles, other financial services and users' friends and family," said Alex Holden, the founder of Hold Security, which has been tracking the flow of stolen Yahoo credentials on the underground web. "This is one of the biggest breaches of people's privacy and very far-reaching."[2]

26. Other reports indicate that this was the largest data breach from a single site in history.

27. The consequences of the Yahoo data breach will be significant, and the breach demonstrates that the Company has, by acting with reckless disregard for the security of its users'

[2] Nicole Perlroth, *Yahoo Says Hackers Stole Date on 500 Million Users in 2014*, N.Y. TIMES (Sept. 22, 2016).

personal information that it promised to protect, utterly failed to implement reasonable security measures to protect its users' sensitive personal information, despite the Company being the target of data breaches in the past. As a result of Defendants' reckless conduct and failure to establish and implement basic data security protocols, despite their knowledge and the warnings of prior data breaches, its users' personal information is now in the hands of criminals, subjecting Plaintiff and the Class to the serious risk of identity theft in a wide variety of forms.

28. What is worse, despite the fact that the attack took place in late 2014, Yahoo was so reckless in securing its users' personal information that it says that it did not even discover the incident until the summer of 2016 – ***nearly two years after the attack***. This is an unusually long time to identify a hacking incident. Indeed, according to the Ponemon Institute, which tracks data breaches, the average time it takes organizations to identify a data breach is 191 days, and the average time to contain a breach is 58 days after discovery.[3]

Yahoo's Recommended Security Steps

29. In Yahoo's September 22, 2016 press release announcing the attack, the Company provided a link to a Yahoo Account Security Notice.

30. Also available after following the link provided in the press release was a page detailing Account Security Issues Frequently Asked Questions ("FAQs"). The FAQs provided additional background on the data breach and offered suggestions on how Yahoo users could secure their account.

31. One recommendation was that users place a "security freeze" (also known as a "credit freeze") on their credit files. A security freeze is designed to prevent potential creditors from accessing an individual's credit file at the consumer reporting agencies without the individual's consent, and costs roughly between $5 and $20 per freeze. The Company provided instructions on how to implement a security freeze and provided additional details on what the security-freeze process entails, but offered no financial assistance.

[3] *Id.*

32. Moreover, adding insult to injury, upon information and belief, when a Yahoo account holder contacts Yahoo as a result of being unable to access their hacked account, Yahoo or its technician representatives advise them that they must pay several hundred dollars for "security protection" in order to unlock and gain access to their account.

33. On Monday, September 26, 2016, Plaintiff was forced to pay $150 for one year of security protection to Global Soft Systems in order to access her Yahoo account and protect her computer from criminals. Plaintiff, and other Class members who do the same and for other damages, should be compensated by Yahoo for the cost of the security freeze, credit protection, and/or identity theft protection in light of Yahoo's reckless failure to adequately secure its users' personal information.

PLAINTIFF'S EXPERIENCE

34. Plaintiff, an Australian citizen, has been a Yahoo user continually for over 10 years and has been damaged as a result of the data breach that Yahoo announced on September 22, 2016.

35. Unable to gain access to her Yahoo account on Monday, September 26, 2016, Plaintiff contacted Yahoo directly. A Yahoo representative confirmed that Plaintiff's account had been hacked by "Russians," and told Plaintiff that in order to gain access to her Yahoo account, she would have to pay $150 for one of year of security protection. Feeling like she had no choice, Plaintiff paid Global Soft Systems $150.

CLASS ACTION ALLEGATIONS

36. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 ("Rule 23") on behalf of herself and a class of other similarly situated individuals (the "Class"), as defined specifically below:

> **All persons residing in the country of Australia whose personal information was accessed following the data breach that Yahoo announced in a press release on September 22, 2016**.

37. Excluded from the Class are Defendant; any person who is an officer, director, partner or controlling person of Defendant, including any of its subsidiaries or affiliates; any entity in which Defendants have a controlling interest; and the legal representatives, heirs, successors and assigns of any such excluded person or entity.

38. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy prerequisites for suing as a representative party pursuant to Rule 23.

39. **Numerosity**. Yahoo has stated publicly that approximately 500 million of its users were affected by this data breach worldwide, and, upon information and belief, millions of users reside in Australia alone. Joinder is therefore impracticable and the numerosity requirement of Rule 23 is easily satisfied here.

40. **Commonality**. Plaintiff's and Class members' claims raise predominately common factual and legal questions that can be answered for all Class members through a single class-wide proceeding. For example, to resolve any Class member's claims, it will be necessary to answer the following questions, and the answer to each of these questions will necessarily be the same for each Class member.

(a) whether Defendant owed a duty of care to Plaintiff and the Class with respect to the security of their personal information;

(b) whether Defendant acted with reckless disregard for the safety and security of the personal information it promised to protect by failing to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against known and anticipated threats or hazards to the security and integrity of these records;

(c) whether the Defendant's conduct was reckless or intentional;

(d) whether Defendant acted appropriately in securing Plaintiff and Class members' personal information; and

(e) whether Plaintiff and Class members are entitled to damages.

41. **Typicality**. Plaintiff's claims are typical of the claims of the members of the Class. Among other things, Plaintiff and Class members provided personal information that was stored on Defendant's systems because they are users of Yahoo's services. In addition, Plaintiff's claims are typical of Class members' claims as each arises from the same data breach and the same alleged reckless conduct on the part of Yahoo in handling the Class members' personal information.

42. **Adequacy**. Plaintiff will adequately represent the proposed Class members. She has retained counsel competent and experienced in class action and privacy litigation and intends to

pursue this action vigorously. Plaintiff has no interests contrary to or in conflict with the interests of Class members.

43. In addition to satisfying the prerequisites of Rule 23(a), Plaintiff satisfies the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual members and a class action is superior to individual litigation. Plaintiff knows of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action.

COUNT I

Gross Negligence

44. Plaintiff incorporates the above allegations by reference.

45. By maintaining their personal information in a database that was accessible through the Internet, Yahoo owed Plaintiff and Class members a duty of care to employ reasonable Internet security measures to protect this information.

46. Defendant, with reckless disregard for the safety and security of users' personal information it was entrusted with, breached the duty of care owed to Plaintiff and the Class by failing to implement reasonable security measures to protect its users' sensitive personal information. In failing to employ these basic and well-known Internet security measures, Yahoo departed from the reasonable standard of care and violated its duty to protect Plaintiff's and Class members' personal information. Defendant further breached its duty of care by allowing the breach to continue undetected and unimpeded for nearly two years after the hackers first gained access to Defendant's systems.

47. The unauthorized access to Plaintiff's and Class members' personal information was reasonably foreseeable to Yahoo, particularly considering that the method of access is widely known in the computer and data security industry, and that it has long been standard practice in the Internet technology sector to encrypt personal information, including critical login credentials.

48. Neither Plaintiff nor other Class members contributed to the security breach or Yahoo's employment of insufficient security measures to safeguard personal information.

49. As a direct and proximate cause of Yahoo's reckless conduct, Plaintiff and Class members suffered injury through the public disclosure of their personal information, the unauthorized access to Internet accounts containing additional personal information, and through the heightened risk of unauthorized persons stealing additional personal information. Plaintiff and Class members have also incurred the cost of taking measures to identify and safeguard accounts put at risk by disclosure of the personal information stolen from Yahoo, including placing a security freeze on their credit file and paying for security protection from computer intrusions.

COUNT II

Bailment

50. Plaintiff incorporates the above allegations by reference.

51. Plaintiff and members of the Class delivered their personal information to Yahoo for the exclusive purpose of creating a Yahoo account.

52. In delivering their personal and financial information to Yahoo, Plaintiff and Class members intended and understood that Yahoo would adequately safeguard their personal information.

53. Yahoo accepted possession of Plaintiff's and Class members' personal information for the purpose of creating a Yahoo user account.

54. By accepting possession of Plaintiff's and Class members' personal information, Yahoo understood that Plaintiff and Class members expected Yahoo to adequately safeguard their personal information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

55. During the bailment (or deposit), Yahoo owed a duty to Plaintiff and Class members to exercise reasonable care, diligence and prudence in protecting their personal information.

56. Yahoo breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' personal information, resulting in the unlawful and unauthorized access to and misuse of their personal information.

57. Yahoo further breached its duty to safeguard Plaintiff's and Class members' personal information by failing to timely and accurately notify them that their information had been compromised as a result of the Yahoo data breach.

58. As a direct and proximate result of Yahoo's breach of its duty, Plaintiff and Class members suffered consequential damages that were reasonably foreseeable to Yahoo, including but not limited to the damages set forth herein.

59. As a direct and proximate result of Yahoo's breach of its duty, the personal information of Plaintiff and Class members entrusted to Yahoo during the bailment (or deposit) was damaged and its value diminished.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Maria Corso, on behalf of herself and the Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class, and appointing her counsel as Class Counsel;

B. Awarding damages to Plaintiff and Class members in an amount to be determined at trial;

C. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

D. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

E. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

DATED: September 29, 2016

ROBBINS GELLER RUDMAN
& DOWD LLP
SHAWN A. WILLIAMS

s/ Shawn A. Williams
SHAWN A. WILLIAMS

Post Montgomery Center
One Montgomery Street, Suite 1800
San Francisco, CA 94104
Telephone: 415/288-4545
415/288-4534 (fax)

ROBBINS GELLER RUDMAN
& DOWD LLP
PAUL J. GELLER
STUART A. DAVIDSON
JASON H. ALPERSTEIN
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)

LABATON SUCHAROW LLP
JOEL H. BERNSTEIN
CORBAN S. RHODES
ROSS M. KAMHI
140 Broadway, 34th Floor
New York, NY 10005
Telephone: 212/907-0700
212/818-0477 (fax)

Attorneys for Plaintiff Maria Corso

I:\Admin\CptDraft\Other\Cpt Yahoo! Data Breach_Corso.docx